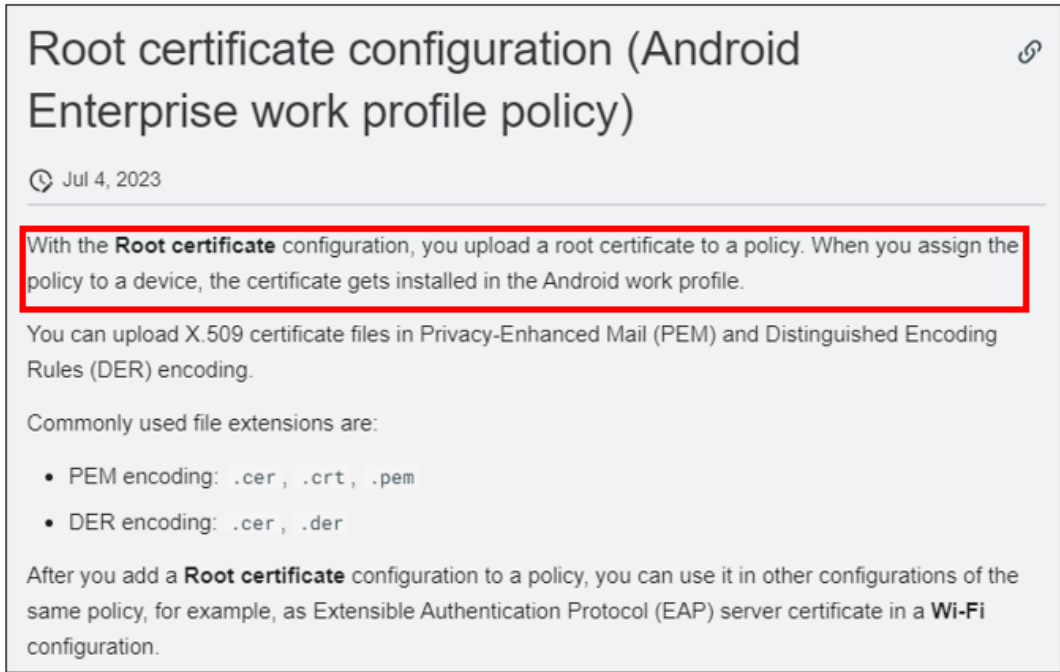


Exhibit 10

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

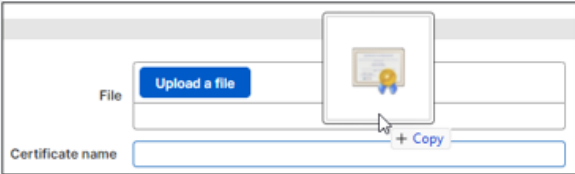
Exhibit 10 – U.S. Patent No. 9,426,145

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
<p>[1pre] A method of creating a certificate store in a memory of a device, the method comprising:</p>	<p>Sophos Mobile is used to create a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="690 524 1743 1192">  <p>Root certificate configuration (Android Enterprise work profile policy)</p> <p>Jul 4, 2023</p> <p>With the Root certificate configuration, you upload a root certificate to a policy. When you assign the policy to a device, the certificate gets installed in the Android work profile.</p> <p>You can upload X.509 certificate files in Privacy-Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) encoding.</p> <p>Commonly used file extensions are:</p> <ul style="list-style-type: none"> • PEM encoding: .cer , .crt , .pem • DER encoding: .cer , .der <p>After you add a Root certificate configuration to a policy, you can use it in other configurations of the same policy, for example, as Extensible Authentication Protocol (EAP) server certificate in a Wi-Fi configuration.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

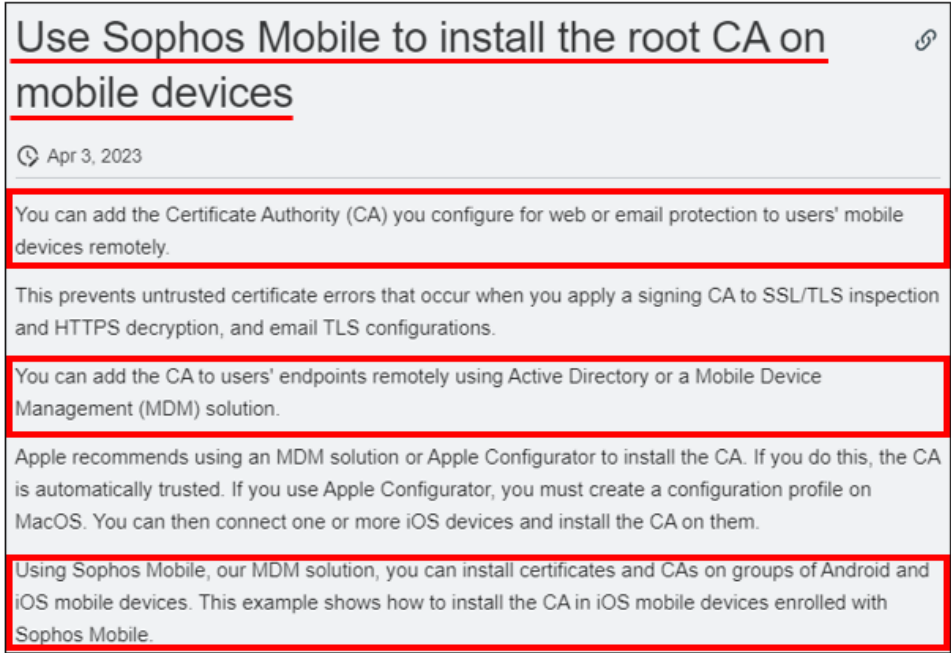
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p>Sophos Mobile is used to create a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="810 383 1619 1097"> <p>Upload certificate</p> <p>For a general description of adding configurations to a policy, see Create policy.</p> <p>To upload a root certificate to a policy, do as follows:</p> <ol style="list-style-type: none"> 1. On the policy's Edit policy page, click Add configuration > Root certificate. 2. Click Upload a file. 3. Select a file containing a certificate in X.509 format and click Open. <p>Tip: Instead of using Upload a file, you can drag the certificate file from File Explorer and drop it anywhere in the File area.</p>  <ol style="list-style-type: none"> 4. After the file is uploaded, the Certificate name field shows the certificate issuer's Distinguished Name (DN) information. <p>Certificate name: CN=*.dialogs.de, O=Sophos Technology GmbH, L=Karlsruhe, ST=E</p> <ol style="list-style-type: none"> 5. Click Apply to save the configuration. 6. On the Edit policy page, click Save. <p>To upload more root certificates, add a Root certificate configuration for each certificate to the policy.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 318 1879 378">Sophos Mobile is used to create a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="741 427 1686 1076">  <p data-bbox="751 443 1560 540"><u>Use Sophos Mobile to install the root CA on mobile devices</u></p> <p data-bbox="751 570 884 594">Apr 3, 2023</p> <p data-bbox="751 630 1640 683">You can add the Certificate Authority (CA) you configure for web or email protection to users' mobile devices remotely.</p> <p data-bbox="751 711 1675 764">This prevents untrusted certificate errors that occur when you apply a signing CA to SSL/TLS inspection and HTTPS decryption, and email TLS configurations.</p> <p data-bbox="751 792 1556 846">You can add the CA to users' endpoints remotely using Active Directory or a Mobile Device Management (MDM) solution.</p> <p data-bbox="751 873 1675 959">Apple recommends using an MDM solution or Apple Configurator to install the CA. If you do this, the CA is automatically trusted. If you use Apple Configurator, you must create a configuration profile on MacOS. You can then connect one or more iOS devices and install the CA on them.</p> <p data-bbox="751 987 1667 1073">Using Sophos Mobile, our MDM solution, you can install certificates and CAs on groups of Android and iOS mobile devices. This example shows how to install the CA in iOS mobile devices enrolled with Sophos Mobile.</p> </div> <p data-bbox="611 1133 1829 1187">https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Certificates/HowToArticles/CertificatesInstallRootCAUsingSophosMobile/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification						
	<p data-bbox="611 318 1843 375">Sophos Mobile is used to create a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="709 459 1732 1120"> <p data-bbox="722 475 1491 581">Client certificate configuration (Android Enterprise work profile policy)</p> <p data-bbox="722 613 871 638">Feb 13, 2023</p> <p data-bbox="722 675 1675 732">With the Client certificate configuration you install a client certificate onto devices. This certificate is available to managed Google Play apps, i.e. to apps installed in the work profile.</p> <p data-bbox="722 764 1688 821">The certificate is available to other configurations of the same policy. If you require certificates in other policies, you must upload them again.</p> <table data-bbox="722 849 1650 1112"> <thead> <tr> <th>Setting</th><th>Description</th></tr> </thead> <tbody> <tr> <td>File</td><td>Select Upload a file and then select a PKCS #12 (.pfx) certificate file.</td></tr> <tr> <td>Certificate name</td><td>The name of the certificate. Sophos Mobile reads the name from the certificate file.</td></tr> </tbody> </table> </div> <p data-bbox="611 1141 1789 1166">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/ClientCert/index.html</p>	Setting	Description	File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.	Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.
Setting	Description						
File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.						
Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.						

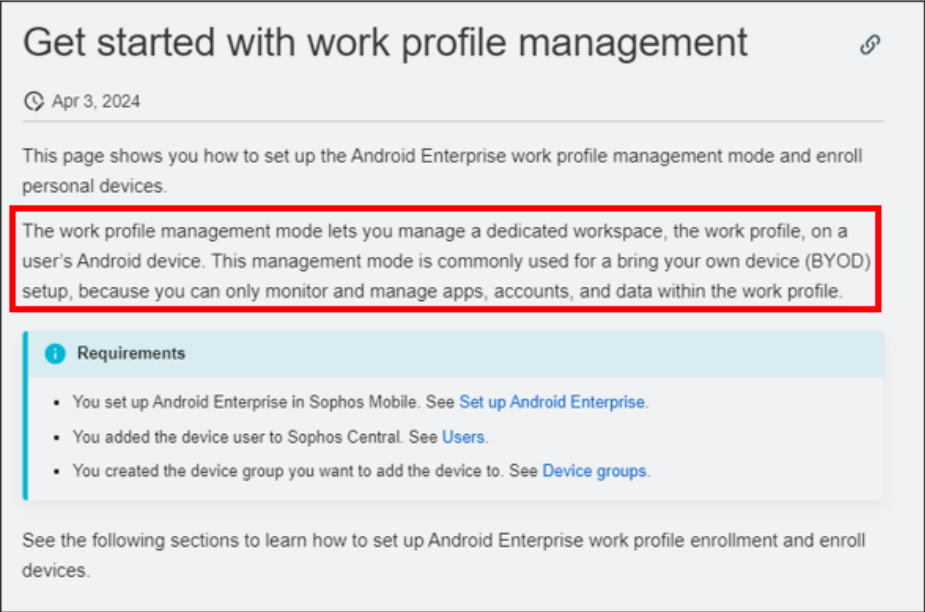
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p>Sophos Mobile is used to create a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div><h3>SCEP configuration (Android Enterprise work profile policy) </h3><p> Feb 13, 2023</p><p>With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to apps that are installed in the work profile.</p></div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/SCEP/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
<p>[1a] receiving, at a space management module, a command to create a memory space, the memory space associated with a designation of a class identifying a first mode of operation of the device, such that data in the memory space can not be accessed by applications executed on the device when the device is operating in a second mode of operation;</p>	<p>With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (i.e., a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (i.e., a second mode of operation).</p>  <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p>With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="640 581 1829 870"> </div> <div data-bbox="747 933 1690 1109"> <h3>Work Profile</h3> <p>Separate work apps and data (managed by your organization) from employee personal data on employee and company-owned devices.</p> </div> <p>https://www.android.com/enterprise/work-profile/</p>

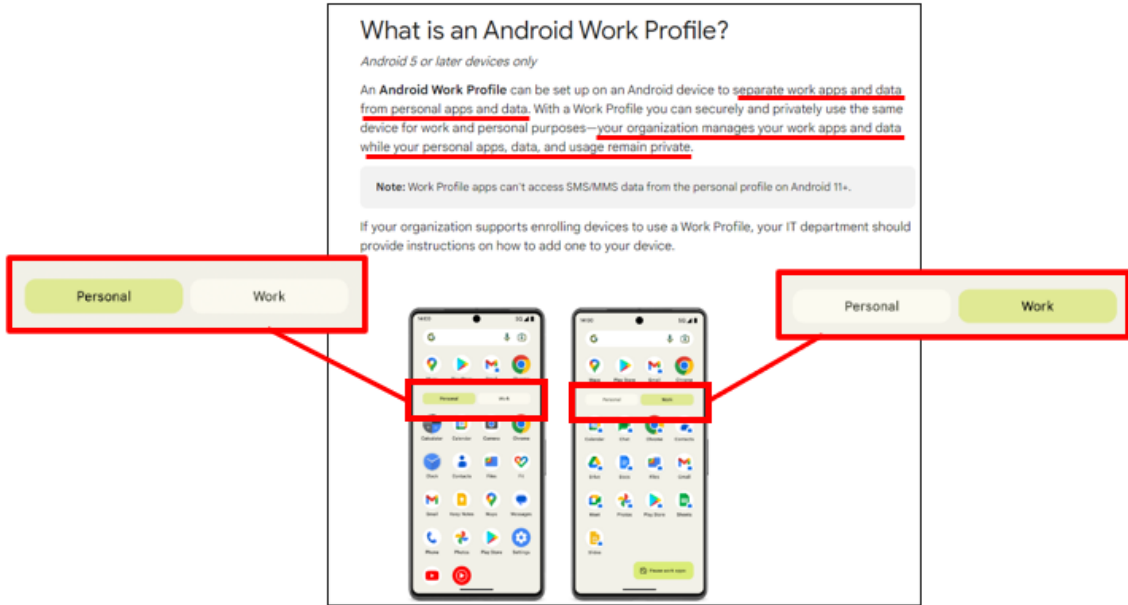
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="617 289 1892 415">With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="699 537 1808 982" style="border: 2px solid red; padding: 10px;"> <p data-bbox="741 565 1344 613">Work Profile and its features</p> <p data-bbox="741 634 1776 841"><u>A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage.</u> On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device’s personal profile and overall device behavior.</p> <p data-bbox="741 865 1764 964">Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile.</p> </div> <p data-bbox="617 1092 1808 1154">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 285 1887 412">With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="655 493 1776 1094">  <p>The diagram illustrates the concept of an Android Work Profile. It features a title 'What is an Android Work Profile?' followed by a subtitle 'Android 5 or later devices only'. The main text explains that an Android Work Profile can be set up on an Android device to separate work apps and data from personal apps and data. It states that with a Work Profile, users can securely and privately use the same device for work and personal purposes, with the organization managing work apps and data while personal apps, data, and usage remain private. A note specifies that Work Profile apps can't access SMS/MMS data from the personal profile on Android 11+. Below the text, two smartphone screens are shown. The left screen displays a 'Personal' tab (highlighted with a red box) and a 'Work' tab (highlighted with a red box). The right screen displays a 'Personal' tab (highlighted with a red box) and a 'Work' tab (highlighted with a red box). Red arrows point from the 'Work' tab on the left screen to the 'Work' tab on the right screen.</p> </div> <p data-bbox="611 1130 1476 1162">https://support.google.com/work/android/answer/6191949?hl=en</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p>With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="699 509 1780 1091" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><u>Data segregation</u></p> <p><u>Work profiles use the following data segregation rules.</u></p> <p>Apps </p> <p>When the same app exists in the primary user and work profile, <u>apps are scoped with their own segregated data</u>. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold <code>INTERACT_ACROSS_PROFILES</code> permission or App-ops.</p> <p>Accounts</p> <p>Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p> <p>Intents</p> <p>The administrator controls whether intents are resolved in or out of the work profile. <u>By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</u></p> </div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="615 282 1892 410">With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="709 555 1795 852"><p data-bbox="745 581 1713 690">What policies is my organization enforcing on my device?</p><p data-bbox="745 711 1755 841"><u>If your device has a work profile, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization.</u> Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned.</p></div> <p data-bbox="726 1133 1780 1159">https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="615 321 1890 448">With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="648 662 1797 846"><p data-bbox="676 678 953 719">Work profile </p><p data-bbox="1644 691 1757 708">Send feedback</p><p data-bbox="676 760 1757 833">The work profile solution set is intended for employee-owned devices and company-owned devices for work and personal use. <u>Corporate apps, data, and management policies are restricted to the work profile.</u> With a work profile, the same device can be used securely and privately for work and personal purposes.</p></div> <p data-bbox="615 1092 1556 1125">https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 321 1900 448">With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="798 485 1709 1115" style="border: 1px solid black; padding: 10px;"> <p data-bbox="840 500 1503 524">What policies can my organization manage on my device?</p> <p data-bbox="840 544 1659 686">When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p data-bbox="840 708 1612 760">If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul data-bbox="840 781 1663 1115" style="list-style-type: none"> • <u>Remotely create, access, and delete data in your work profile</u> • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • <u>Restrict what can be shared across your work and personal profiles</u> • <u>Block screen captures in your work profile</u> • <u>Manage access to your organization's corporate mail server and internal data</u> • <u>Remotely install (and uninstall) apps and certificates in your work profile</u> • <u>Manage permissions and other settings for apps in your work profile</u> </div> <p data-bbox="655 1182 1856 1206">https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification																
	<p>With Android Enterprise Work Profile managed by Sophos Mobile, a space management module creates memory space and associates it with a “work” profile (<i>i.e.</i>, a first mode of operation) to store data and apps such that data in the memory space can not be accessed by applications associated with a “personal” profile (<i>i.e.</i>, a second mode of operation).</p> <div data-bbox="787 503 1669 1071"> <p>Device management</p> <table> <tr> <th>Feature</th><th>Description</th></tr> <tr> <td>Manage Google Workspace accounts</td><td>Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td>Manage 3rd party certificates</td><td>Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td>Control access to input methods</td><td>Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles</td></tr> <tr> <td>Control access to accessibility services</td><td>Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td>Set location sharing preferences</td><td>Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td>Disable screen captures</td><td>Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td>Retrieve network statistics</td><td>Retrieve network usage statistics for a Work Profile.</td></tr> </table> </div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																


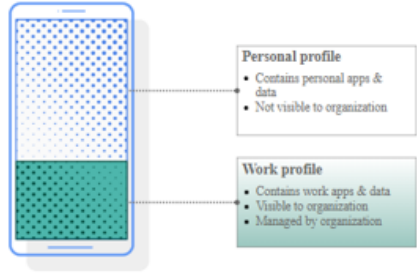
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
<p>[1b] designating, at the space management module, a range of addresses in a memory for the memory space; and</p>	<p>With Android Enterprise Work Profile managed by Sophos Mobile, the space management module designates a range of addresses in a memory for work profile memory spaces.</p> <div data-bbox="705 542 1770 906"> <p>Securing work data</p> <p><u>Separation between a user's personal data and work data is enforced at the OS kernel level across processes, memory and storage.</u> All applications from Google Play work out of the box with separate data storage and there's no need for modification of applications.</p> </div> <p>https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_One_Pager_BYOD.pdf</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 280 1875 342">With Android Enterprise Work Profile managed by Sophos Mobile, the space management module designates a range of addresses in a memory for work profile memory spaces.</p> <div data-bbox="703 378 1780 1096"> <p data-bbox="720 394 1220 418">Android devices: management use cases ⇄</p> <p data-bbox="720 451 1749 496">This section describes the management options available in Android to support managed deployments. You can use Android Enterprise's tools and services to support any or all of the following options in your EMM solution.</p> <p data-bbox="720 537 1230 561">  Work profile for employee-owned devices (BYOD) </p>  <p data-bbox="1045 881 1444 901">Figure 1. Personally-owned device with a work profile.</p> <p data-bbox="720 922 1764 993">BYOD devices can be set up with a work profile—a feature built into Android 5.1+ <u>that allows work apps and data to be stored in a separate, self-contained space within a device.</u> An employee can continue to use their device as normal; all their personal apps and data remain on the device's primary profile.</p> <p data-bbox="720 1016 1764 1088">An employee's organization has full management control of the apps, data, and settings in their device's work profile, but has no visibility or access to the device's personal profile. This distinct separation gives organizations control over corporate data and security without compromising employee privacy.</p> </div> <p data-bbox="1045 1130 1535 1154">https://developers.google.com/android/work/overview</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 318 1887 380">With Android Enterprise Work Profile managed by Sophos Mobile, the space management module designates a range of addresses in memory for work profile memory spaces.</p> <div data-bbox="611 493 1887 805"> <p data-bbox="644 513 863 548">Work profiles</p> <p data-bbox="644 581 1860 781">You can manage a user's business data and applications through a work profile. A work profile is a managed corporate profile associated with the primary user account on an Android device. A work profile securely isolates work apps and data from personal apps and data. <u>This work profile is in a separate container from the personal profile, which your user controls.</u> These separate profiles allow organizations to manage the business data they care about, but leave everything else on a user's device under the user's control. For a deep dive into best practices, see the Work profiles guide. For an overview of those best practices, see below.</p> </div> <p data-bbox="980 813 1396 837">https://developer.android.com/work/guide</p> <div data-bbox="611 932 1887 1052"> <ul style="list-style-type: none"> <li data-bbox="636 948 1860 1044">• <u>Since the personal and work profiles have separate storage areas, a file URI that is valid on one profile is not valid on the other.</u> Any intent fired on one profile might be handled on the other (depending on profile settings), so it is not safe to attach file URIs to intents. </div> <p data-bbox="995 1062 1526 1086">https://developer.android.com/work/managed-profiles</p>

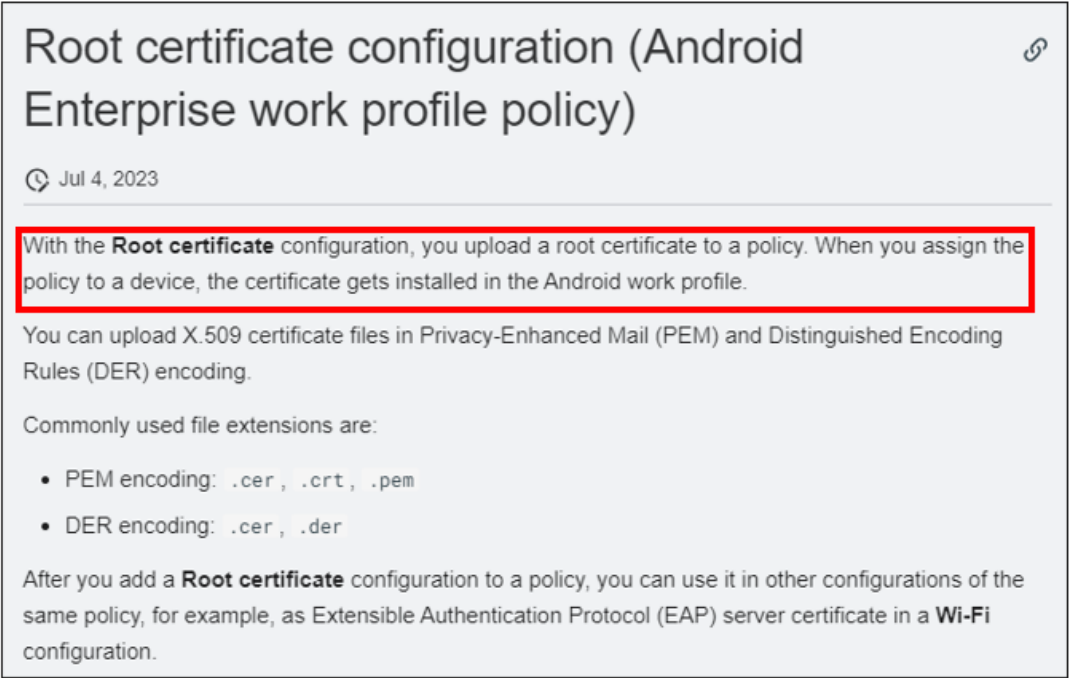
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="617 280 1881 342">With Android Enterprise Work Profile managed by Sophos Mobile, the space management module designates a range of addresses in memory for work profile memory spaces.</p> <div data-bbox="617 496 1881 1029"><h2 data-bbox="653 524 1470 581">Data and file storage overview </h2><p data-bbox="653 638 1860 699">Android uses a file system that's similar to disk-based file systems on other platforms. The system provides several options for you to save your app data:</p><ul data-bbox="684 730 1871 1019" style="list-style-type: none"><li data-bbox="684 730 1871 829">• App-specific storage: Store files that are meant for your app's use only, either in dedicated directories within an internal storage volume or different dedicated directories within external storage. Use the directories within internal storage to save sensitive information that other apps shouldn't access.<li data-bbox="684 854 1871 915">• Shared storage: Store files that your app intends to share with other apps, including media, documents, and other files.<li data-bbox="684 940 1346 971">• Preferences: Store private, primitive data in key-value pairs.<li data-bbox="684 995 1671 1026">• Databases: Store structured data in a private database using the Room persistence library.</div> <p data-bbox="1020 1128 1524 1154">https://developer.android.com/training/data-storage</p>

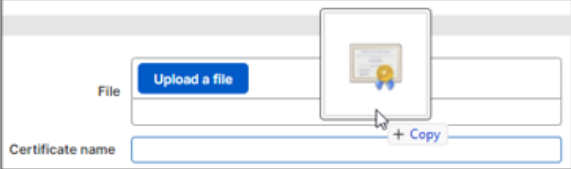
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
<p>[1c] initializing, at a certificate manager, a certificate store in the memory of the device, the certificate store associated with the designation of the class.</p>	<p>Sophos Mobile is used to initialize a certificate store (e.g., to store root and other certificates) in the memory of a device in association with an Android work profile.</p> <div data-bbox="695 443 1757 1117">  <p>Root certificate configuration (Android Enterprise work profile policy)</p> <p>Jul 4, 2023</p> <p>With the Root certificate configuration, you upload a root certificate to a policy. When you assign the policy to a device, the certificate gets installed in the Android work profile.</p> <p>You can upload X.509 certificate files in Privacy-Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) encoding.</p> <p>Commonly used file extensions are:</p> <ul style="list-style-type: none"> • PEM encoding: .cer , .crt , .pem • DER encoding: .cer , .der <p>After you add a Root certificate configuration to a policy, you can use it in other configurations of the same policy, for example, as Extensible Authentication Protocol (EAP) server certificate in a Wi-Fi configuration.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

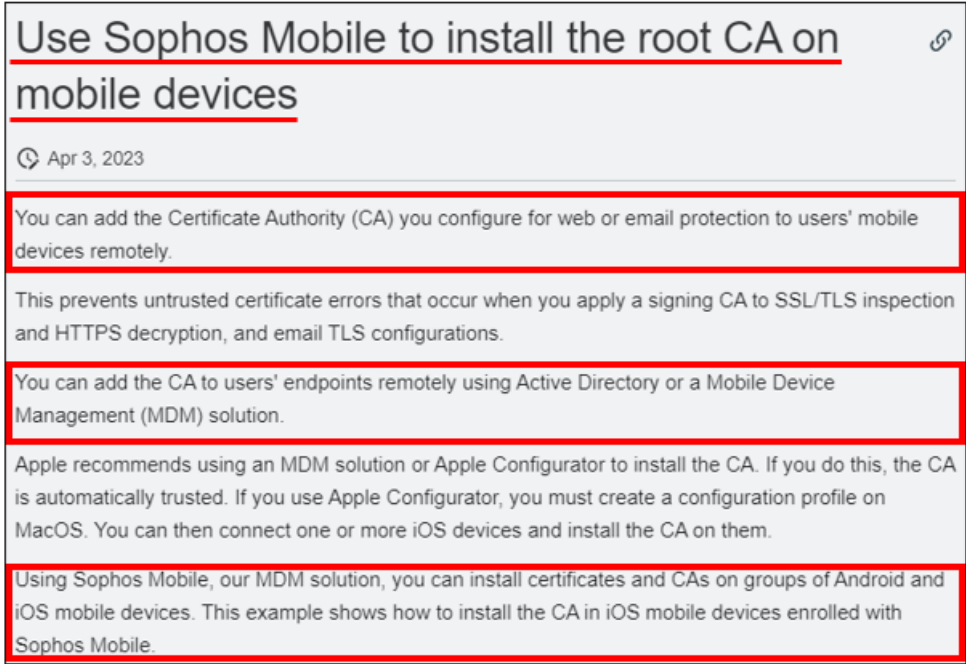
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 318 1871 378">Sophos Mobile is used to initialize a certificate store (e.g., to store root and other certificates) in the memory of a device in association with an Android work profile.</p> <div data-bbox="829 410 1633 1123"> <p data-bbox="850 423 1087 456">Upload certificate</p> <p data-bbox="850 480 1423 500">For a general description of adding configurations to a policy, see Create policy.</p> <p data-bbox="850 521 1226 540">To upload a root certificate to a policy, do as follows:</p> <ol data-bbox="865 561 1444 649" style="list-style-type: none"> <li data-bbox="865 561 1444 581">1. On the policy's Edit policy page, click Add configuration > Root certificate. <li data-bbox="865 594 1024 613">2. Click Upload a file. <li data-bbox="865 626 1367 646">3. Select a file containing a certificate in X.509 format and click Open. <p data-bbox="884 662 1583 708">Tip: Instead of using Upload a file, you can drag the certificate file from File Explorer and drop it anywhere in the File area.</p>  <ol data-bbox="865 906 1570 1078" style="list-style-type: none"> <li data-bbox="865 906 1570 951">4. After the file is uploaded, the Certificate name field shows the certificate issuer's Distinguished Name (DN) information. <li data-bbox="865 1024 1150 1044">5. Click Apply to save the configuration. <li data-bbox="865 1057 1150 1076">6. On the Edit policy page, click Save. <p data-bbox="850 1097 1583 1117">To upload more root certificates, add a Root certificate configuration for each certificate to the policy.</p> </div> <p data-bbox="611 1162 1801 1185">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

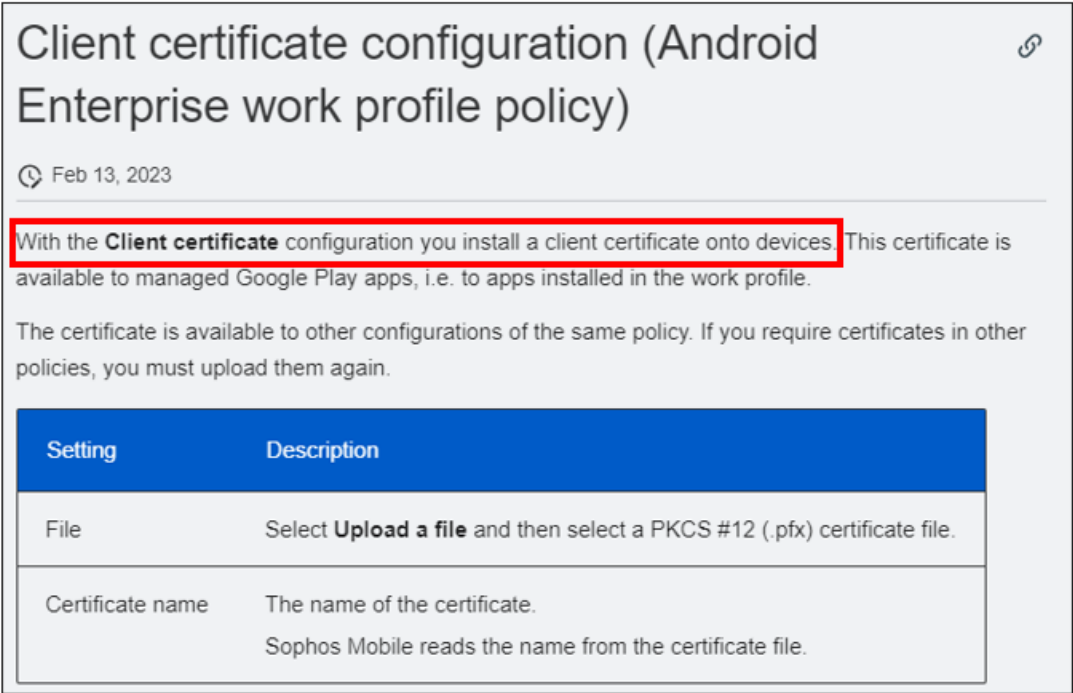
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 318 1894 380">Sophos Mobile is used to initialize a certificate store (e.g., to store root and other certificates) in the memory of a device in association with an Android work profile.</p> <div data-bbox="758 428 1717 1088">  <p>The screenshot shows a help article with the title "Use Sophos Mobile to install the root CA on mobile devices" and a date of "Apr 3, 2023". The article contains several paragraphs, some of which are highlighted with red boxes. The highlighted text includes: "You can add the Certificate Authority (CA) you configure for web or email protection to users' mobile devices remotely.", "This prevents untrusted certificate errors that occur when you apply a signing CA to SSL/TLS inspection and HTTPS decryption, and email TLS configurations.", "You can add the CA to users' endpoints remotely using Active Directory or a Mobile Device Management (MDM) solution.", "Apple recommends using an MDM solution or Apple Configurator to install the CA. If you do this, the CA is automatically trusted. If you use Apple Configurator, you must create a configuration profile on MacOS. You can then connect one or more iOS devices and install the CA on them.", and "Using Sophos Mobile, our MDM solution, you can install certificates and CAs on groups of Android and iOS mobile devices. This example shows how to install the CA in iOS mobile devices enrolled with Sophos Mobile."</p> </div> <p data-bbox="611 1143 1850 1198">https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Certificates/HowToArticles/CertificatesInstallRootCAUsingSophosMobile/index.html</p>



Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification						
	<p data-bbox="615 282 1896 342">Sophos Mobile is used to initialize a certificate store (e.g., to store root and other certificates) in the memory of a device in association with an Android work profile.</p> <div data-bbox="714 428 1780 1117">  <p data-bbox="726 444 1528 558">Client certificate configuration (Android Enterprise work profile policy)</p> <p data-bbox="726 586 884 613">Feb 13, 2023</p> <p data-bbox="726 651 1722 716">With the Client certificate configuration you install a client certificate onto devices. This certificate is available to managed Google Play apps, i.e. to apps installed in the work profile.</p> <p data-bbox="726 743 1734 808">The certificate is available to other configurations of the same policy. If you require certificates in other policies, you must upload them again.</p> <table border="1" data-bbox="726 833 1692 1109"> <thead> <tr> <th>Setting</th><th>Description</th></tr> </thead> <tbody> <tr> <td>File</td><td>Select Upload a file and then select a PKCS #12 (.pfx) certificate file.</td></tr> <tr> <td>Certificate name</td><td>The name of the certificate. Sophos Mobile reads the name from the certificate file.</td></tr> </tbody> </table> </div> <p data-bbox="615 1138 1839 1166">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/ClientCert/index.html</p>	Setting	Description	File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.	Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.
Setting	Description						
File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.						
Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.						

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 10 – U.S. Patent No. 9,426,145

Claims	Identification
	<p data-bbox="611 280 1885 342">Sophos Mobile is used to initialize a certificate store (e.g., to store root and other certificates) in the memory of a device in association with an Android work profile.</p> <div data-bbox="709 500 1751 849"><p data-bbox="722 521 1738 634">SCEP configuration (Android Enterprise work profile policy) </p><p data-bbox="722 662 879 690"> Feb 13, 2023</p><p data-bbox="722 727 1724 824">With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to apps that are installed in the work profile.</p></div> <p data-bbox="611 1130 1776 1157">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/SCEP/index.html</p>